finiz
Singidunum University International Scientific Conference
Međunarodna naučna konferencija Univerziteta Singidunum

BANKING
Professional work - prospective study

BITCOIN - BANKING AND TECHNOLOGICAL CHALLENGES

Goran Kunjadić,
Zoran Jović

Singidunum University,
Belgrade, Serbia

Abstract:
Indisputable exponential growth of the Internet use in modern banking and stock exchange operations is the basic trend in the financial industry. Important aspects of the bitcoin problem include the area for its use, the factors that influence its price, and regulatory aspects in different countries. There is also a dilemma as to whether bitcoin should be considered money or goods. In technological terms, bitcoin was realized using an open source which is available to anyone and the system is not officially in anyone's possession or under anyone's control. Bitcoin uses peer-to-peer technology that works without the interference of the central bank or commercial banks. Managing transactions and broadcasting of bitcoin is performed by the network itself. The system is not based on trust of the participants, but on the distributed control system. The issue that should be particularly addressed is the security management of a virtual currency. The authors shall propose a new way of encryption which can significantly enhance both the privacy and security segment. Thus, conclusions can be drawn that the use of bitcoin poses new challenges to the banking system, and opens up many dilemmas that the authors shall attempt to process in this paper.

Keywords:
bitcoin, virtual currency, security, encryption.

INTRODUCTION

Bitcoin is a currency that allows parties to exchange value, as was the case with the paper money and gold. However, unlike the previous currency, bitcoin is the first decentralized digital currency. For the first time in history, bitcoin can exchange value without intermediaries, allowing for greater control of resources and lower fees. Bitcoin is a form of a non-centralized digital currency, *i.e.*, purchased data mining process via P2P networks. Earned *i.e.* excavated coins can be used to pay for goods or services on the Internet, as well as for resale purposes. Bitcoin is quite changeable and varies depending on the state of supply and demand in the market. We record a constant increase in the number of sites that receive bitcoin billing. Opinions seem to be divided as regards the future of bitcoin, since many call it a new bubble-like tulip bubble. A ledger-based system using the same technology but with the valuation fixed to an existing fiat currency, such as USD, or perhaps a commodity such as gold, might offer a more secure future for bitcoin or lead to its end.

Bitcoin can be used in a way that solves computer algorithms hidden behind the data. Since there is no central bank to regulate the value of individual coins and their price depends merely on the supply and demand, large fluctuations of the bitcoin value can be observed. The absence of a central bank also causes the problem of lack of credit and interest rates, which is necessary to let the currency, including bitcoin, to be considered the right currency. One of the problems in the functioning of bitcoin is the fact that it is not subject to state regulations, but can buy the products on the Internet that are illegal in some countries, and may be involved in money laundering operations and

Correspondence:
Goran Kunjadić

e-mail:
gkunjadic@singidunum.ac.rs

DOI: 10.15308/finiz-2016-185-189

terrorism financing. On the other hand, bitcoin is impossible to counterfeit, as it is not subject to the tax system of domestic markets, transactions are relatively anonymous, self coins can be exchanged for various currencies and sent anywhere in the world in real time, and at no cost (Jovic, 2014).

Blockchain is a major bitcoin technical innovation serving as the joint public book relying on the entire bitcoin network. All confirmed transactions are included in the blockchain. In this way, we can track the status of the funds in bitcoin wallets and it can be verified by a new transaction that spends bitcoin property of their holder. The integrity and chronological order of the blockchain are enforced with cryptography. Blokchain is not some kind of bank, but a system that records and provides the most reliable data on bitcoin transactions. It has no insight into the individual bitcoin accounts, cannot see the owners of bitcoin transactions and make payments on their behalf. It carries a record of completed transactions and balances bitcoin through a series of graphs. Blockchain has certain characteristics of many forex trading platforms for currency pairs, but because of the specificity of bitcoin and its physical limitations, it simultaneously carries specificity of universal platform for the historical record of all transactions and the total volume of the decentralized digital currency. Graphical presentations are divided into several categories which show: Currency statistics, Block details, Mining information, Network activity, Blockchain Wallet Activity. In the category Currency statistics, the charts display the following: Total number of bitcoin ever excavated, e.i., the current quote on the bitcoin network; The movement and the current market price of bitcoin in US dollars calculated as the average market price of bitcoin expressed in USD based on the large bitcoin transactions (exchange); The market capitalization calculated by multiplying the total amount of bitcoin in circulation and the daily average market price for big exchanges; The volume of trade expressed in USD, which represents the value of the total trading volume on the main bitcoin exchanges. Other categories of charts dedicated to Blockchain database are divided into: the block showing the details such as Blockchain Size, Average Block Size, Orphaned Blocks, Blocks per Transaction, Transaction Confirmation Median Time; Mining Information that shows Rate Hash, Hash Rate Distribution, Difficulty, Mining Revenue, Total Transaction Fees, % Cost of Transaction Volume, Cost per Transaction; Network activity - a set of charts relating to the blockchain network; Blockchain Wallet Activity related to the users of Blockchain Wallet and their total number.

BANKING CHALLENGES

A bitcoin payment is faster, cheaper, safer and less volatile than the local currencies in many countries. Therefore, it can be used in these countries for storing values, besides being used to pay for many products and services around the world and on the Internet. There are also certain challenges concerning the use of bitcoin.

Regulatory aspects

The regulatory authorities of certain countries react differently to bitcoin. For instance, China's central bank has banned the trade and bitcoin payment for financial institutions and other legal entities, but not for individuals, while German law formally recognized the existence of bitcoin payment method, which means that the bitcoin payment method is subject to the statutory tax liability and the corresponding sanctions for non-compliance with tax law (Jovic, 2014b).

There are also examples of Iceland, which restricts money being sent abroad, Vietnam, where all electronic currencies are illegal, Ecuador, which has banned cryptocurrencies while they conduct a review on introducing their own (O'Grady, 2014) and Bolivia, which has banned all currencies not issued by the government or an authorized entity (Rizzo, 2014). Ultimately, lost tax revenues and potential use of bitcoin in illegal activities are the factors most likely to drive regulators to draw up legislation in the near future.

Factors that influence the price

The proportion of bitcoins that have been bought and held is around 90%. Because of that, the only transactions that we see on the market relate to the purchase of newly mined bitcoins and actual payments being made with the remaining 10%. This relatively low level of active usage will have a serious impact on bitcoin liquidity and is likely to be one of the key causes of price volatility. A low daily turnover makes the price susceptible to large-sized transactions such that one investor, with a reasonable sized holding of bitcoin, selling their stake could have an immediate negative effect on the price or vice versa. There sometimes appear that the most rapid changes in the USDBTC currency pair price are associated with concomitant variations in the volume of transactions. The fact that rapid increases in price do seem to have an effect of increasing demand for bitcoin, would add weight to the argument that there is an element of speculation in bitcoin. Considering data supports, we can conclude that bitcoin is uncorrelated with the rest of the market and the volume of transactions only affects the price, or vice versa, while in extreme situations, other factors must be causing the considerable volatility. Low liquidity is likely a factor, but the market sentiment seems to have the greatest effect. Market announcements such as a large retailer accepting bitcoin or, conversely, a regulator introducing legislation that bans or limits the use of cryptocurrencies in a particular jurisdiction could have a substantial impact on the market sentiment and affect the price.

Bitcoin: Currency or commodity?

The lack of clarity over bitcoin's status in the market from a regulatory perspective is widespread with only few bodies such as the US Inland Revenue Service (IRS), the US Treasury's Financial Crimes Enforcement Network (FinCEN) (Little 2014) and Finland's central bank (Pohjanpalo, 2014) giving direct guidance. The ruling of the IRS was that bitcoins should be classified as a property from a tax perspective. FinCEN acknowledged that those who exchange or administer transmission of bitcoin should be considered "money transmitters", which has implications for banking secrecy regulations. Finish National Bank's stated view was made as follows: "Considering the definition of an official currency as set out in law, it's not that. It's also not a payment instrument, because the law stipulates that a payment instrument must have an issuer responsible for its operations". Thus, it can be concluded that it is more comparable to a commodity at this stage". The Finnish National Bank is not alone in holding this view.

From a simplistic perspective, for something to be considered an effective currency, it should have two key characteristics: it should be widely accepted and should represent an effective store of value in some way. The features of bitcoin are not valid for currencies. Conversely, if we look at an archetypal commodity, such as gold, we see significant parallels in their characteristics. If bitcoin were to be considered a currency in a government's jurisdiction, then the government would eventually take action to resist its competition to the government backed currency. This might take a form of legislation outlawing its use in transactions, imposition of taxes that must be paid in the local fiat currency or a requirement for increased levels of information on remitter and beneficiary in line with anti-money laundering standards. There is no doubt that significant similarities exist between the asset class and bitcoin. While many authors were asserting that bitcoin is not a currency and were struggling to categorically state that it should be classified as a commodity, some authors explain this dichotomy of bitcoin action by claiming that bitcoin is as a speculative financial asset that can be used as a medium of exchange.

Field of use

The profile of the current bitcoin usage appears dominated by speculators who have bought and are holding bitcoin. This practice reduces the overall liquidity and increases volatility. If bitcoin is to be successful as a payment system, there must be a shift to more transactional users so that the price is stabilized. The characteristics of bitcoin do not match those of other currencies, but rather its ability to store and transfer value is indicative that it should be more correctly categorized as a commodity. High volatility may ultimately limit its usefulness unlike commodities such as gold due to the lack of price stability.

TECHNOLOGICAL CHALLENGES

Bitcoin is a new form of digital currency. Instead of being released by a central bank, its distribution is controlled by a decentralized computer network. The network consists of numerous servers deployed worldwide. This network relies on network technology and cryptography to regulate the "virtual printing" of bitcoins and who owns the "virtual cash". Because of that, bitcoin is known as a cryptocurrency. Notwithstanding this, bitcoin uses a ledger and it is kept up collaboratively by the decentralized computer network. That is why it is also called a distributed ledger. As new transaction enrollment is added to this distributed ledger, they attach references back to the previous groups of records. All participants can verify for themselves the source and origin of every record on the ledger. These groups of transaction entries forming blocks, and the collection of blocks are called a block chain. The originator of the blockchain, Satoshi Nakamoto, said that it was a system of "purely peer-to-peer electronic cash" which can be fully controlled by the owner. Furthermore, bitcoin can be sent to anybody without needing permission of the bank or taking a risk a confiscation. Each participant in the bitcoin system has a copy of every single transaction, arranged in these blocks. The owner can go all the way back to the start of the bitcoin. Each block is linked to the previous block using the cryptographic mechanism, thus forming a block chain. The block chain shows a full history of transactions. Every single copy of the ledger is synchronized by mathematical algorithms which are keeping consistency about the state of the ledger. Still, once a transaction is properly confirmed, it cannot be reversed. Various software applications are developed for accessing the ledger. The applications can be used on various devices including mobile phones, tablet, computers *etc.*

As the user needs to store and transfer bitcoins, special software, called bitcoin wallet, has to be used. Bitcoin wallet can be considered a virtual bank account. There are two main types of wallets. The first one is software wallet that the user installs on own smart device. The owner of bitcoin has complete control over the security of coins, but these wallets can be difficult to install and maintain. The second one is Web wallet, or hosted wallet. The Web wallet is hosted by a third party. They are definitely easier to use, but the user must believe that the Internet service provider is able to ensure a high level of security to protect virtual money.

Current crypto solution

The current crypto solution used for bitcoin crypto protection is Elliptic curve cryptography algorithm. The Elliptic

curve cryptography or ECC is used to protect many contemporary systems, such like crypto protection of iPhone and iPad devices. The ECC is more advanced than RSA (Rivest Shamir Adleman) asymmetric cryptographic algorithm. It is proven that breaking of the ECC is much harder and requires significantly more resources and time then breaking RSA. The RSA is still used in banking chip card technology, so it is less secure then bitcoin encryption. The quality of the ECC algorithm relies on the fact that in the ECC algorithm, the random point of elliptic curve is used instead of the random integer number in RSA algorithm. The ECC is far from perfect and has known weakness. There are several most commonly used attacks on ECC crypto systems such as: Pohlig-Hellman attack, Pollard's rho attack, Parallelized Pollard's rho attack, Index-calculus attacks, Isomorphism attacks, Attack on prime-field-anomalous curves, Weil and Tate pairing attacks *etc*.

The RSA algorithm uses Public key infrastructure or PKI as well as ECC. PKI system implies the existence of Certification authority or CA. The Certification authority is a dedicated entity that is generating and distributing pairs of cryptographic keys. Also, the Certification authority guarantees the user identity. Without CA the identity of the user could not be reliably confirmed. So, CA has access to the cryptographic data of the users and can forge identity or reveal the data about the bitcoin wallet of any user.

Based on the above-listed arguments, we can conclude that the ECC does not guarantee user privacy even if the Satoshi Nakamoto claims this. This implies that ECC is vulnerable and does not guarantee privacy.

The question arises as to what could be the solution to this issue.

Proposed solution

The authors propose a more appropriate cryptographic solution: Identity Based Encryption or IBE. The IBE solution relies on the symmetric cryptography but with the specific key generation. The solution uses a set of keys to provide the functioning of the system. The keys are generated using parameters provided by the user. It could be any string that is known only by the user itself. Strings have to satisfy the defined requirements and after that convert to binary or hexadecimal. The user can create own keys locally or entrust the key creation to trusted center. After that, only the derived keys are used for securing the data. If the keys are compromised, the user can simply create the new ones. The option is also to use new keys for every new record in the blockchain. Thus, the security of the bitcoin encryption significantly increases.

The appearance of certificate-less authenticated encryption (CLAE) scheme, as an encryption scheme that uses the identity strings to provide identity-based encryption. The CLAE solution offers a way to configure a PKI system in the way that digital certificates and certificate authorities are no longer needed. Thus, we eliminated the need for distributing and managing public keys using the PKI system. If CLAE is used, the public keys can be generated and verified locally. Once the system is initialized, any entity in the system can self-generate the public key of other entities. The user can encrypt bitcoin data using the recipient's identity. The recipient's identity string could be whatever the user chooses, converted to binary or hexadecimal number. In the proposed system, only the true recipient is able to decrypt and retrieve the sensitive data using a private key known only to the recipient and obtained from a trusted center.

The main advantage of the proposed solution is elimination of certification authorities and rising the privacy of bitcoin user to a higher level.

CONCLUSION

Bitcoin is a cryptocurrency that brings challenges in banking as well as technology. Virtual currency is a currency without a country and interference of the central bank or commercial banks. Security of information system and distributed database that support bitcoin are a huge challenge. The paper provides a short overview of the complexity of the bitcoin system, from the perspective of banks and data security. We analyze the current crypto mechanism and point out to its shortcomings.

If implemented, our proposition could significantly improve the security and privacy segment of bitcoin usage. Also, further research is needed that would highlight some other aspects.

REFERENCES

Antonopoulos, A.M. (2014). *Mastering Bitcoin: Unlocking, Digital Cryptocurrencies*. Sebastopol, CA: O'Reilly Media.

Baek, J., Wong, D.S., Li, J., Au, M.H. (2016). Efficient Generic Construction of CCA-Secure Identity-Based Encryption from Randomness Extraction. *The Computer Journal*, 59(4), 508-521. doi:10.1093/comjnl/bxv070

Chaudhry, S.A., Farash, M.S., Naqvi ,H., & Sher, M. (2016). *A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography*. Electronic Commerce Research, 16: 113. doi:10.1007/s10660-015-9192-5

Fournaris, A.P., Papachristodoulou, L., Batina, L., & Sklavos N., (2016). *Residue Number System as a side channel and fault injection attack countermeasure in elliptic curve cryptography*. IEEE Design and Technology of Integrated Systems in Nanoscale Era (DTIS).

Jovic, Z. (2014). *Aplication of information technology in the financial performance of non-cash transations*. Zbornik radova, VI naučni skup sa međunarodnim učešćem: Mreža 2014, Valjevo, 08.05.2014.

Jovic, Z. (2014b).*The use of the Internet in modern banking and stock exchange activities*. Zbornik radova, Međunarodna naučna konferencija Sinteza 2014, Beograd 25-26.04.2014.

Little, E.M. (2014). Bitcoin. *The Investment Lawyer*, 21(5), 22-26.

Liu, Z., Seo, H., Grosschadl, J., & Kim H. (2016). Efficient Implementation of NIST-Compliant Elliptic Curve Cryptography for 8-bit AVR-Based Sensor Nodes. *IEEE Transactions on Information Forensics and Security*, 11(7). doi: 10.1109/TIFS.2015.2491261

Malek B. (2013). *Method and system for a certificate-less authenticated encryption scheme using identity-based encryption*. United States Patent, US 2013/0212377 A1

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Available from https://bitcoin.org/bitcoin.pdf

O'Grady M. (2014). Ecuador's Phony Bitcoin Ploy. *Wall Street Journal*. Available from http://www.wsj.com (Accessed 25 January 2015).

Perez-Marco, R. (2016). *Bitcoin and Decentralized Trust Protocols*. Ithaca, USA: Cornell University Library.

Pohjanpalo, K. (2014). Bitcoin Judged Commodity in Finland After Failing Money Test. *Bloomberg,* 20 January. Available from http://www.bloomberg.com (Accessed 25 January 2014).

Rizzo, P. (2014). *Bolivia's Central Bank Bans Bitcoin*. Available from http://www.coindesk.com (Accessed 15 June 2015).

Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. Sebastopol, CA: O'Reilly Media.

UK Government Chief Scientific Adviser. (2016). *Distributed ledger technology: beyond block chain*. UK Government Office For Science.

BITKOIN - BANKARSKI I TEHNOLOŠKI IZAZOVI

Apstrakt:

Neosporni eksponencijalni porast upotrebe interneta u modernom bankarstvu i berzanskim operacijama predstavlja dominantan trend u razvoju finansijske industrije. Postoji nekoliko važnih problema kada je reč o korišćenju bitkoina - obim njegove upotrebe, formiranje cene usled dejstva brojnih faktora, pravna regulativa u različitim zemljama i najzad ključna dilema da li bitkoin treba posmatrati kao novac ili kao robu? U tehnološkom smislu, bitkoin je otvoreni izvor koji je dostupan bilo kome i kao sistem zvanično nije ničija svojina i nije ni pod čijom kontrolom. Bitkoin koristi P2P tehnologiju koja funkcioniše bez uplitanja centralne banke ili komercijalnih banaka. Upravljanje transakcijama i prenošenje bitkoina vrši se preko same mreže. Sistem se ne zasniva na poverenju učesnika već na raspoloživom kontrolnom sistemu. Upravljanje sistemom virtualne valute predstavlja zaseban problem. U ovom radu predlažemo novi način šifrovanja koji u značajnoj meri može unaprediti privatnost, a istovremeno uvećati i stepen bezbednosti korišćenja bitkoina. Upotreba bitkoina donosi nove izazove za bankarski sistem kakvim ga mi znamo i otvara mnoge dileme koje ćemo pokušati da obradimo u ovom radu.

Ključne reči:

bitkoin,
virtualna valuta,
bezbednost,
šifrovanje.